证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003.11.06

申　请　号：　2003101142548

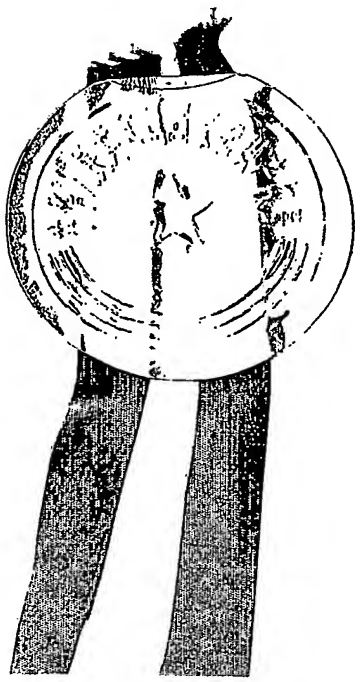
IB/04/52278

申请类别：　发明

发明创造名称：　一种解密光盘的方法和系统

申　请　人：　皇家飞利浦电子股份有限公司

发明人或设计人：　彭扬



中华人民共和国
国家知识产权局局长　王景川

2004 年 10 月 10 日

权 利 要 求 书

1、一种解密光盘的方法，包括步骤：

a．向服务器发出一个请求，所述请求要求服务器提供解密光盘的信息；

b．接收来自服务器的解密信息，所述解密信息包括两层数据，第一层包含与光盘不可复制的数据相关的信息，第二层包含解密光盘的方法；

c．根据所述第一层的信息从光盘中获取不可复制的数据，并用来解密第二层的信息，从而获得用于解密光盘的方法及其相关参数；和

d．用步骤 c 中获得的结果解密光盘。

2、如权利要求 1 所述的方法，其中所述请求包括所述光盘的主题信息。

3、如权利要求 1 所述的方法，还包括步骤，向服务器发送用于播放器的身份识别信息，供服务器对播放器进行身份识别。

4、如权利要求 1 所述的方法，还包括步骤，获得所述解密信息后，将其储存在本地存储空间中。

5、一种生成光盘解密信息的方法，包括步骤：

a. 接收到来自播放器的要求解密光盘的请求；

b. 从预存的数据中选取所要播放光盘的不可复制的数据，所述预存的数据包括与要播放的光盘相对应的数据；

c. 将所述不可复制的数据对用于解密光盘的方法及其相关参数加密，得到加密结果；和

d. 将获得所述不可复制数据的方法和所述加密结果发送给播放器。

6、如权利要求 5 所述的方法，其中步骤 b 中从所述预存的数据中获取不可复制的数据是随机进行的。

7、如权利要求 5 所述的方法，其中所述不可复制的数据包括下述至少一种数种：版权管理信息(Copyright Management Information , CPR_MAI)、光盘物理格式信息、光盘制造信息、光盘上脉冲串切割区（Burst Cutting Area，BCA）中的信息。

8、如权利要求 5 所述的方法，其中步骤 d 中获取不可复制数据的方法的内容，包括所述不可复制数据所在扇区的位置及长度。

9、一种解密光盘的装置，包括：

一个发送装置，用于向服务器发送一个请求，要求服务器提供解密光盘的信息；

一个接收装置，用于接收来自服务器的解密信息，所述解密信息包括两层数据，第一层包含与光盘不可复制的数据相关的信息，第二层包含解密光盘的方法；

一个解密数据获取装置，用于根据所述第一层的信息从光盘中获取不可复制的数据，并用来解密第二层的信息，从而获得用于解密光盘方法及其相关参数；及

一个解密装置，用所述的用于解密光盘方法及其相关参数来解密光盘。

10、如权利要求 9 所述的装置，其中所述发送装置发送的请求中包括光盘的主题信息。

11、如权利要求 9 所述的装置，所述发送装置还用于发送用于播放器的身份识别信息，供服务器对播放器进行身份识别。

12、如权利要求 9 所述的装置，还包括一个存储装置，用于存储所述的解密信息。

13、一种光盘播放器，包括：

一个光盘读取装置，用于读取光盘信息，该光盘信息包括光盘内容；

一个光盘播放装置，用于播放所述的光盘内容；和

一个光盘解密装置，用于解密光盘，该光盘解密装置包括：

一个发送装置，用于向服务器发送一个请求，要求服务器提供解密光盘的信息；

一个接收装置，用于接收来自服务器的解密信息，所述解密信息包括两层数据，第一层包含与光盘不可复制的数据相关的信息，第二层包含解密光盘的方法；

一个解密数据获取装置，用于根据所述第一层的信息从光盘中获取不可复制的数据，并用来解密第二层的信息，从而获得解密光盘的方法及其相关参数；及

一个解密装置，用所述解密光盘的方法及其相关参数来解密光盘。

14、一种生成光盘解密信息的装置，包括：

一个接收装置，接收来自播放器的要求解密光盘的请求；

一个选取装置，从预存的数据中选取所要播放的光盘的不可复制的数据，所述预存的数据包含与要播放的光盘相对应的数据；

一个加密装置，将所述不可复制的数据对用于解密光盘的方法及其相关参数加密，得到加密结果；及

一个发送装置，将获得所述不可复制数据的方法和所述加密结果发送给播放器。

15、如权利要求 14 所述的装置，其中所述选取装置随机选取光盘的不可复制的数据。

16、如权利要求 14 所述的装置，其中所述不可复制的数据包含下述至少一种数据：版权管理信息(Copyright Management Information , CPR_MAI)、光盘物理格式信息、光盘制造信息和光盘上脉冲串切割区（Burst Cutting Area，BCA）中的信息。

说 明 书

一种解密光盘的方法和系统

背景技术

本发明涉及一种解密光盘的方法和系统，尤其涉及一种从互联网中获取解密光盘信息的方法和系统。

目前当内容提供者用光盘发布内容时，该光盘系统能否提供充分的复制保护是他们关心的问题。很多光盘格式采用了不同的复制保护方法，例如 DVD-Video（DVD 视频）的 内容加密系统（Content Scrambling System ，CSS），DVD-Audio(DVD 音频)的对预记录媒体的内容保护（Content Protection for Pre-recorded Media，CPPM），以及 CD2 的 Sapphire 系统。通常，这些方案使用加密系统，内容密钥被储存在光盘的安全区域，只有经过授权许可并验证的播放器才能取得密钥并正确解密光盘内容。上述这些方案都是在播放器本地使用的，不能在互联网中使用。而且，目前 CSS 系统已经被破解了。而 CPPM 系统仅限于 DVD 音频使用。

图 1 是现有的从互联网中获得光盘解密信息的系统示意图。播放器 130 开始播放光盘 120 后，向服务器 140 请求用于解密光盘的解密信息，服务器 140 通过网络接收到该请求后，向播放器 130 发送解密信息，播放器 130 用该解密信息解密光盘 120。由于现有技术中只是简单的改变了解密信息的存放位置，从原来存放在光盘中改变到存放在服务器上，因此不能有效的解决解密信息的安全问题。由于新一代光盘播放器建立网络互联是必然的趋势，我们需要一个适合互联网的安全的提供解密光盘信息的方案。

发明内容

本发明提供了一种解密光盘的方法。光盘播放器通过向服务器发出一个请求，从服务器获得可以解密光盘的信息，该信息包括两层数据，第一层是包含与光盘不可复制的数据相关的信息，第二层包含解密光盘的方法；然后根据第一层的信息从光盘中获取不可复制的数据，并用

来解密第二层的信息，从而获得用于解密光盘的方法及其相关参数，最后，用该解密光盘的方法及其相关参数来解密光盘内容以供播放。

本发明还提供了一种生成光盘解密信息的方法，根据来自播放器的请求，从预存的数据中选取所要播放的光盘的不可复制的数据，该预存的数据包括与要播放的光盘相对应的数据，然后将选取的不可复制的数据对用于解密光盘的方法和相关参数加密，得到一个加密结果，再将获得不可复制数据的方法和加密结果一起发送给播放器。

本发明利用了光盘中不可复制的数据加密用以解密光盘的方法及其相关参数，该不可复制的数据是从与正版光盘对应的预存的数据中随机选取的，对每个光盘或者每个主题，每次选取的数据都可能是不同的，因此增加了破解的难度，提高了传输过程中的可靠性。在解密时，只有具有正版光盘，才能够从正版光盘中得到正确的解密光盘的方法及其相关参数，否则无法正确解密，从而有效的防止了光盘盗版和非法复制等行为。

通过参照结合附图所进行的如下描述和权利要求，本发明的其它目的和成就将是显而易见的， 并对本发明也会有更为全面的理解。

附图说明

本发明通过实例的方式，参照附图进行详尽的解释，其中：

图 1 是现有的从互联网中获得光盘解密信息的系统示意图；

图 2 是根据本发明的一个实施例的光盘播放器的结构示意图；

图 3 是根据本发明的一个实施例的生成光盘解密信息的装置的结构示意图；

图 4 是根据本发明的一个实施例的解密光盘的流程图；

图 5 是根据本发明的一个实施例的解密信息的基本结构。

在所有的附图中，相同的参照数字表示相似的或相同的特征和功能。下面参照附图结合实施例对本发明作进一步说明。

具体实施方式

图 2 是根据本发明一个实施例的光盘播放器的结构示意图。该光盘播放器除同现有的光盘播放装置一样，包括一个光盘读取装置 210，用于从光盘上读取信息，一个光盘播放装置 230，用于播放光盘内容，还包括一个光盘解密装置 200，用于解密被加密过的光盘内容。

该光盘解密装置 200 包括一个发送装置 220，该装置用于通过网络发出一个请求，该请求要求服务器提供用于解密光盘的解密信息，该请求中包含待播放的光盘的主题信息，该主题信息来自于光盘读取装置 210；一个接收装置 240，用于接收来自服务器的解密信息，该解密信息包括两层数据，第一层包含与光盘不可复制的数据相关的信息，例如不可复制数据所在的光盘扇区位置及长度；第二层包含解密光盘的方法，即经光盘不可复制数据（或者加密过的光盘不可复制数据）加密过的解密光盘的方法及其相关参数。该解密信息可以电子证书（eticket）的形式在网络中被传输。关于电子证书的结构详见下述。

该解密光盘的装置 200 还包括一个解密数据获取装置 260，根据从接收装置 240 处收到的上述解密信息的第一层信息从光盘读取装置 210 处获取光盘的不可复制的数据，并用来解密第二层的信息，从而获得用于解密光盘的方法及其相关参数；及一个解密装置 280，用解密数据获取装置 260 处获得的用于解密光盘的方法及其相关参数来解密从光盘读取装置 210 发送来的待播放的光盘内容，然后将解密后的光盘内容发送到光盘播放装置 230 进行播放。

图 3 是根据本发明的一个实施例的生成光盘解密信息的装置的结构示意图。生成光盘解密信息的装置 300 包括一个接收装置 320，接收来自播放器的要求解密光盘的请求，该请求中包括要播放的光盘的主题信息；一个选取装置 340，根据接收装置 320 接收到的请求中的信息，在数据库 310 找到相应的预存的数据，该预存的数据包括与待播放的光盘相对应的数据，如待播放的光盘的物理格式信息及其中的数据信息，该预存的数据可以是存储在一个与待播放的光盘相对应的虚拟光盘文件中，亦可存储在与待播放的光盘源之于同一张母盘的正版光盘中。该选取装置 340 从预存的数据中选取所要播放的光盘的不可复制的数据，并且该选取是随机的，每次选取的不可复制的数据都可以是不同的；

该生成光盘解密信息的装置 300 还包括一个加密装置 360，用于将选取装置 340 发送来的不可复制的数据对用于解密光盘的方法及其相关参数加密，得到一个加密结果；及一个发送装置 380，用于将获得不可复制数据的方法和加密装置 360 发送来的加密结果发送给播放器。

图 4 是根据本发明的一个实施例的解密光盘的流程图。在播放器端，光盘放入播放器中（S400），播放器判断光盘内容是否是经过加密的（S402），如果光盘内容未加密，则正常播放光盘内容（S434）；如果光盘内容是经过加密的，则播放器判断用户是否需要为该内容付费（S406），如果用户选择不付费，则结束；如果用户选择付费，则付费后播放器向服务器提交用于播放器的身份识别信息，并向服务器要求用于解密光盘内容的解密信息 eticket，该请求中包括播放器中光盘的主题信息（S410），以使服务器能够知道播放器正在播放的是哪个光盘。

在服务器端，服务器首先验证步骤 S410 中从播放器发送的身份识别信息是否合法和有效（S412），如果该播放器的身份是非法的，或该播放器的身份有效但已被破解，或者它的请求格式不符合要求，则结束；如果有效且合法，则接受步骤 S410 中播放器发送的要求解密信息的请求（S416）。只有经验证的播放器才可以得到解密信息 eticket。如果发现未通过验证的播放器，服务器可以收回播放器的合法身份证明，即使得该播放器的身份不合法。本发明通过网络中的服务器获取解密光盘内容必需的解密信息 eticket，而未经授权或被破解的(cracked/hacked)播放器将不能得到解密信息 eticket， 这样有利于对播放器权限的回收。

然后服务器根据接收到请求中包含的光盘的主题信息，在服务器的数据库中搜索到与在播放器中待播放的光盘相对应的预存的数据，该预存的数据包括与待播放的光盘相对应的不可复制的数据，如待播放的光盘的物理格式信息及其中的数据信息，该预存的数据可以是存储在一个与待播放的光盘相对应的虚拟光盘文件中，亦可存储在与待播放的光盘源之于同一张母盘的正版光盘中。并从预存的数据中随机选取所要播放的光盘的不可复制的数据（S418），根据选取该不可复制的数据的方法生成解密信息 eticket 中的 A 区信息（详见下述）。

上述提到的光盘不可复制数据可以是以下数据：

1、DVD 光盘上内容提供者信息（Contents Provider Information,CPI）中的版权管理信息（Copyright Management Information,CPR_MAI），它包括复制保护系统和区管理的信息，不可被复制到读写（ RW）盘。

2、光盘物理格式信息 ,如光盘结构，层，区域码等。

3、光盘制造信息，其不可被复制到 RW 盘。光盘物理格式信息和光盘制造信息存在于导入区的控制数据区。

4、DVD 光盘上的脉冲串切割区（Burst Cutting Area, BCA）中的信息。上述提到的四种数据结构在 DVD 光盘标准中都有定义，详见 1997 年 12 月发布在 DVD 论坛的标准文档："只读光盘 DVD 标准－第一部分物理标准"（版本号为 1.01）的第三章。

5、内容提供者储存在光盘上的原始数据，其由逻辑或者物理扇区数和偏移量指示，并且是在 CSS 解密前提取的数据。

当然的，不可复制的数据不限于上述列举的几种。由于是随机选取，原始数据对于每个光盘不必是唯一的，对每个明确的主题也不必是唯一的。得到不可复制的数据后，还可以用特定加密算法如 Hash 算法对光盘不可复制的数据进行加密，也可以不加密，并用该加密或者不加密的不可复制数据对解密光盘的方法及其相关参数（即密码、解密算法及其参数或者密钥等）加密得到加密结果（即 B 区信息，详见下述）(S420)，同时将生成该解密光盘的方法及其相关参数和加密结果存储在电子证书（eticket）中，详见下述。上述 Hash 算法可以是 MD5, SHA-1 等。

在播放器端，播放器判断是否收到解密信息 eticket（S424），如果未收到，则结束，如果收到 eticket，则读取 eticket 中的 A 区信息（S428）。根据 A 区中的信息，如不可复制数据所在的光盘的扇区位置及长度，找到并读取播放器中待播放的光盘中相应位置的不可复制数据，如有需要并用 Hash 算法加密，然后用获取的不可复制数据对 B 区中的信息进行解密，得到解密光盘的方法及其相关参数（密码、解密算法及其参数或者密钥等）（S430）。然后就可以用上述密码、参数、解密算法或者密钥对光盘内容进行解密（S432）。最后，播放解密后的光盘内容（S434）。

图 5 是根据本发明的一个实施例的解密信息的基本结构。该解密信息 eticket 中的信息分两层结构存储，包括明文部分 A 区以及密文部分 B 区。A 区与光盘不可复制的数据相关，而非光盘不可复制数据本身，包括光盘扇区位置及长度，还可以包括加密不可复制数据的加密算法等。B 区是用光盘不可复制数据或者加密的光盘不可复制数据对解密光盘的方法及其相关参数（密码、解密算法及其参数或者密钥）进行加密得到的加密结果。解密信息 eticket 使用了两层结构存储数据，相比于单层结构提高了解密信息 eticket 的传输过程中的保密性和可靠性。而且由于不可复制数据是随机选取的，其随机性大，对于每个光盘或者每个主题，每次选取的数据都可能是不同的，因此增加了破解的难度，大大提高了安全性。

在实际中，为了使光盘可以在将来离线回放(第一次以后)，本实施例也允许服务器中生成的解密信息 eticket 被储存在播放器的存储设备中或者光盘中(如果光盘具有可写区域)。在离线回放光盘时一样需要从原版光盘中获取不可复制的数据对解密信息 eticket 进行解密。

可见本发明中的解密信息 eticket 可以存储在播放器或者光盘中，而不象在其它系统中那样，解密信息只能被严格地限制在播放器的特定的临时内存中。因为解密信息 eticket 中的 B 区信息是与特定的原版光盘相关的，只有当用户同时拥有原版光盘和 eticket 时才可正确解密光盘内容。当有多个 eticket 存在本地空间中时，通过每个光盘主题对应自己的 eticket，可以建立一个光盘与 eticket 的对应关系。

另外,需要解密的内容也不限于光盘中的内容,与光盘有关的内容被下载并存储到本地后也可以用上述的方法进行解密。

虽然经过对本发明结合具体实施例进行描述，对于在本技术领域熟练的人士，根据上文的叙述作出的许多替代、修改与变化将是显而易见的。因此，当这样的替代、修改和变化落入附后的权利要求的精神和范围之内时，应该被包括在本发明中。

说 明 书 附 图

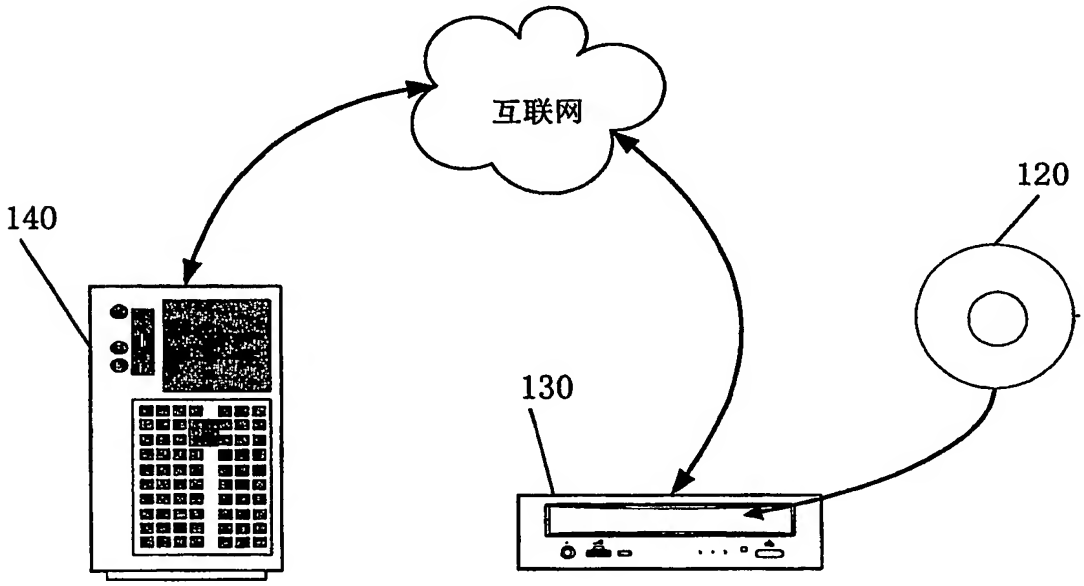


图1

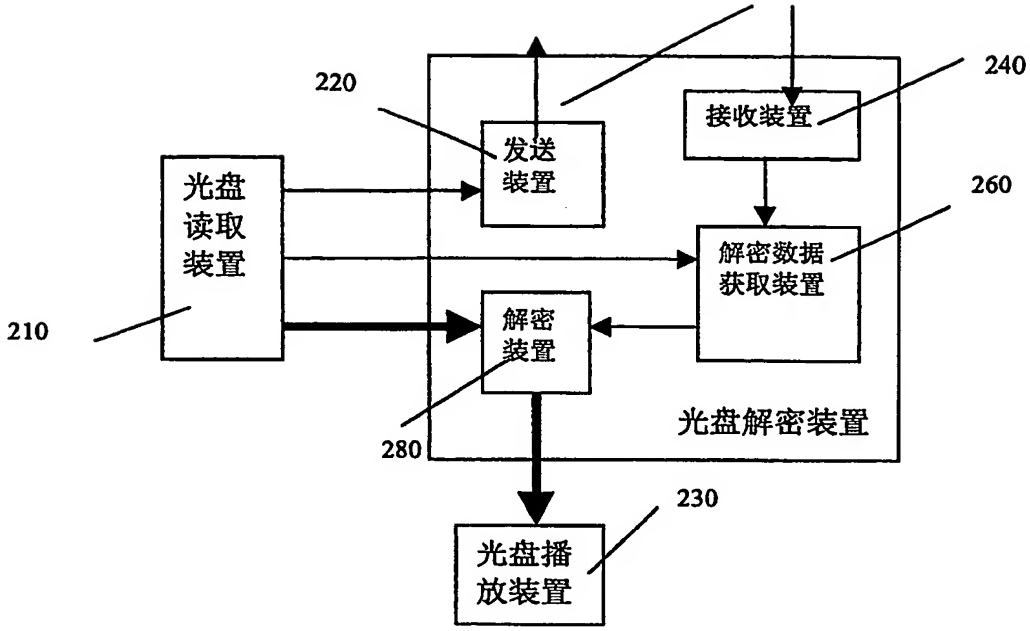

220
240
接收装置
发送
装置
光盘
读取
装置
260
解密数据
获取装置
210
解密
装置
光盘解密装置
280
230
光盘播
放装置

图 2

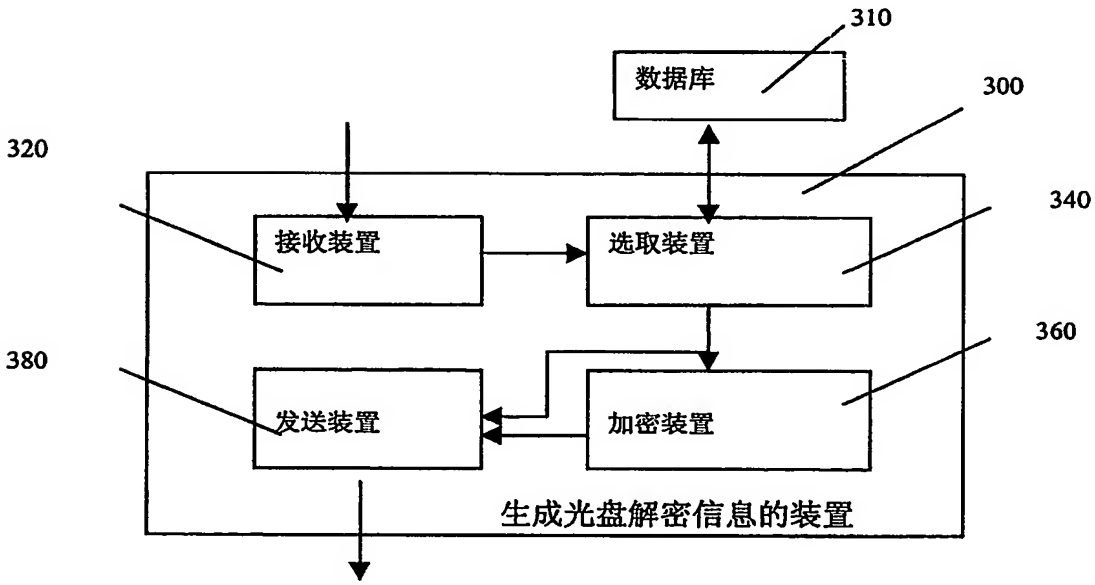

310
数据库
300
320
340
接收装置
选取装置
380
360
发送装置
加密装置
生成光盘解密信息的装置

图 3

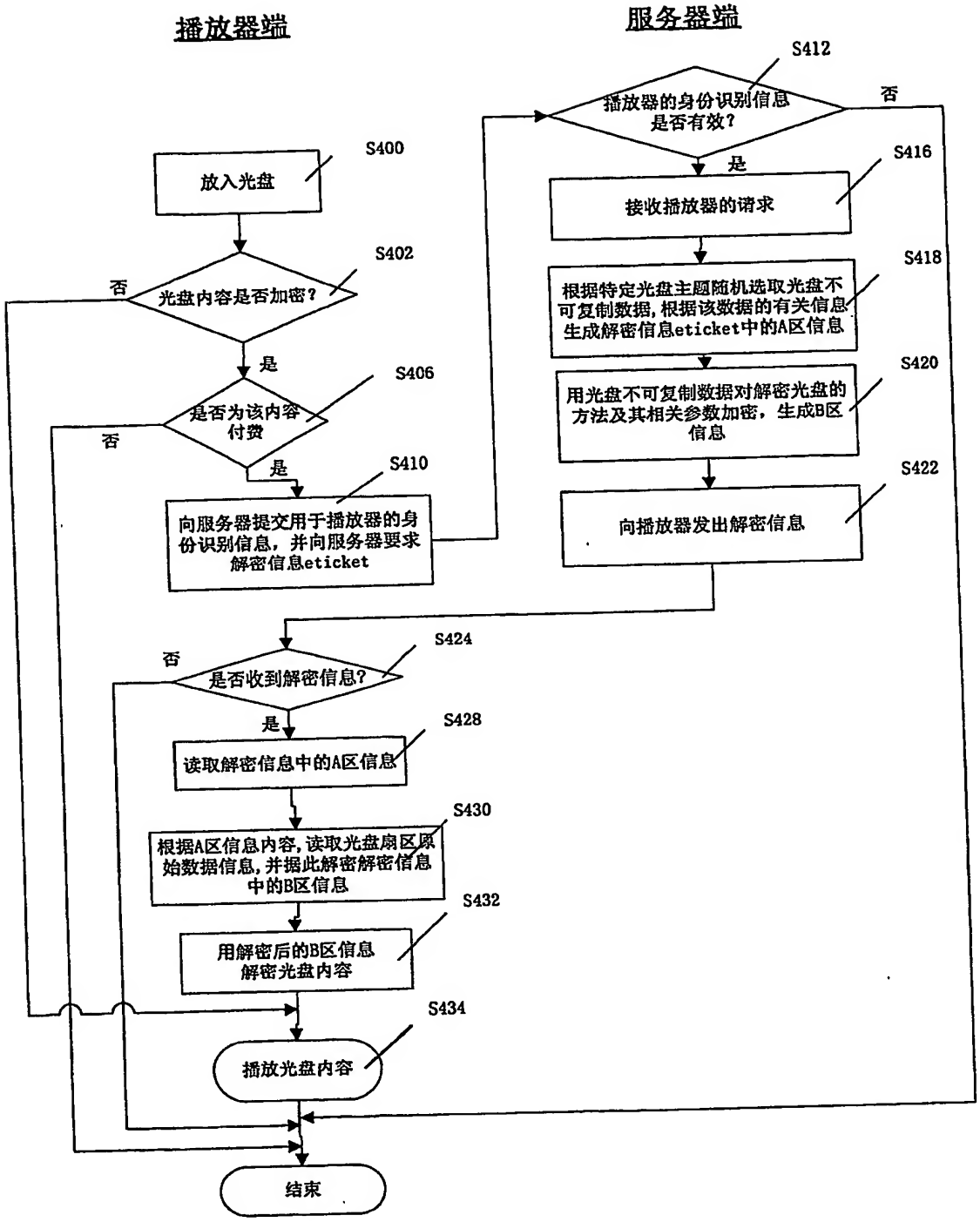

播放器端
服务器端
放入光盘
S400
光盘内容是否加密?
S402
否
是
是否为该内容付费
S406
否
是
S410
向服务器提交用于播放器的身份识别信息，并向服务器要求解密信息eticket
播放器的身份识别信息是否有效?
S412
否
是
S416
接收播放器的请求
S418
根据特定光盘主题随机选取光盘不可复制数据，根据该数据的有关信息生成解密信息eticket中的A区信息
S420
用光盘不可复制数据对解密光盘的方法及其相关参数加密，生成B区信息
S422
向播放器发出解密信息
是否收到解密信息?
S424
否
是
S428
读取解密信息中的A区信息
S430
根据A区信息内容，读取光盘扇区原始数据信息，并据此解密解密信息中的B区信息
S432
用解密后的B区信息解密光盘内容
S434
播放光盘内容
结束

图 4

光盘信息指示 用于获取光盘不可复制数据的的光盘扇区位置和长度信息	明文部分A区
解密数据 由光盘不可复制数据加密的用于解密光盘的方法及其相关参数（密码、解密算法及其参数或者密钥）	密文部分B区

图 5